



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,139	05/22/2001	Roy F. Quick JR.	010055B1	1058
23696 7590 01/24/2008 QUALCOMM INCORPORATED 5775 MOREHOUSE DR. SAN DIEGO, CA 92121			EXAMINER MOORTHY, ARAVIND K	
			ART UNIT 2131	PAPER NUMBER
			NOTIFICATION DATE 01/24/2008	DELIVERY MODE ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com  
kscanla@qualcomm.com  
nanm@qualcomm.com

mv

<b>Office Action Summary</b>	<b>Application No.</b>		<b>Applicant(s)</b>	
	09/863,139		QUICK ET AL.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Aravind K. Moorthy		2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 09 November 2007.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 1-16 and 18-29 is/are allowed.
- 6) ☒ Claim(s) 17 and 30-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

1. This is in response to the arguments filed on 9 November 2007.
2. Claims 1-32 are pending in the application.
3. Claims 1-16 and 18-29 have been allowed.
4. Claim 17 and 30-32 has been rejected.

### ***Response to Arguments***

5. Applicant's arguments with respect to claims 17 and 30-32 have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 17 and 30-32 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The tangible requirement does not necessarily mean that a claim must either be tied to a particular machine or apparatus or must operate to change articles or materials to a different state or thing. However, the tangible requirement does require that the claim must recite more than a Sec. 101 judicial exception, in that the process claim must set forth a practical application of that Sec. 101 judicial exception to produce a real-world result. *Benson*, 409 U.S. at 71-72, 175 USPQ at 676-77 (invention ineligible because had "no substantial practical application."). "[A]n application of a law of nature or mathematical formula to a . . . process may well be deserving of patent protection." *Diehr*, 450 U.S. at 187, 209 USPQ at 8 (emphasis added); see also *Corning*,

56 U.S. (15 How.) at 268, 14 L.Ed. 683 ("It is for the discovery or invention of some practical method or means of producing a beneficial result or effect, that a patent is granted . . ."). In other words, the opposite meaning of "tangible" is "abstract."

Claims 17 and 30-32 are directed towards an apparatus for authenticating a subscriber in a wireless communication system, wherein the apparatus can be communicatively coupled to a mobile station operating within the wireless communications system. They recite generating a primary signature based on a key that is held private from the mobile station and a secondary signature. They recite receiving a secondary signature from a mobile station operating within the wireless communications system. However, nothing is done with either signature. There is no end result with any of the signatures.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

**7. Claims 17 and 30-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Diffie et al U.S. Patent No. 5,371,794.**

As to claim 17, Diffie et al discloses an apparatus for authenticating a subscriber in a wireless communication system, wherein the apparatus can be communicatively coupled to a mobile station operating within the wireless communications system, comprising:

a memory [column 7, lines 3-36]; and

a processor [column 7, lines 3-36] configured to implement a set of instructions stored in the memory [column 7, lines 3-36], the set of instructions for selectively generates a primary signature based upon a key that is held private from the mobile station [column 8 line 26 to column 9 line 7] and a secondary signature that is received from the mobile station [column 8 line 26 to column 9 line 7].

As to claim, Diffie et al discloses a method operational on a device for authenticating a subscriber in a wireless communication system, comprising:

receiving a secondary signature from a mobile station operating within the wireless communications system, wherein the device is configured to be communicatively coupled to the mobile station [column 8 line 26 to column 9 line 7]; and

generating a primary signature based on a key that is held private from the mobile station and the secondary signature [column 8 line 26 to column 9 line 7].

As to claim 31, Diffie et al discloses a device for authenticating a subscriber in a wireless communication system, comprising:

means for receiving a secondary signature from a mobile station operating within the wireless communications system, wherein the device is configured to be communicatively coupled to the mobile station [column 8 line 26 to column 9 line 7]; and

means for generating a primary signature based on a key that is held private from the mobile station and the secondary signature [column 8 line 26 to column 9 line 7].

As to claim 32, Diffie et al discloses a machine-readable medium having one or more instructions operational on a device for authenticating a subscriber in a wireless communication system, which when executed by a processor causes the processor to:

receiving a secondary signature from a mobile station operating within the wireless communications system, wherein the device is configured to be communicatively coupled to the mobile station [column 8 line 26 to column 9 line 7]; and

generating a primary signature based on a key that is held private from the mobile station and the secondary signature [column 8 line 26 to column 9 line 7].

*Allowable Subject Matter*

8. Claims 1-16 and 18-29 are allowed.

As to independent claims 1 and 18-20, prior art does not teach or suggest the limitation “concatenating the initial value with a received signal to form an input value, wherein the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module, and the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit”. Prior art does teach or suggest the limitation “hashing the input value to form an authentication signal“. Prior art does teach or suggest the limitation “transmitting the authentication signal to the communications system via the communications unit”.

As to independent claims 8 and 21-26, prior art does not teach or suggest the limitation “a signature generator configured to receive a secret key from the key generation element and information from a mobile unit, and further configured to generate a signature that will be sent to the mobile unit, wherein the signature is generated by concatenating the secret key with the information from the mobile unit and hashing the concatenated secret key and information [column 8, lines 32-62].

As to independent claims 11 and 27-29, prior art does not teach or suggest the limitation “a key generator for generating a plurality of keys from a received value and a secret value, wherein at least one communication key from the plurality of keys is delivered to the communications unit and at least one secret key from the plurality of keys is not delivered to the communications unit”. Prior art does teach or suggest the limitation “a signature generator for generating an authorization signal from hashing a version of the at least one secret key together with an authorization message that the authorization message is generated by the communications unit using a version of the at least one communication key”.

As to independent claim 15, prior art does not teach or suggest the limitation “generating a plurality of keys”. Prior art does teach or suggest the limitation “transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys”. Prior art does teach or suggest the limitation “generating a signature at the communications device using both the at least one key transmitted to the communications device and a transmission message, wherein generating is implemented by hashing a concatenated value formed from the at least one key and the transmission message”. Prior art does teach or suggest



the limitation “transmitting the signature to the subscriber identification device”. Prior art does teach or suggest the limitation “receiving the signature at the subscriber identification device”. Prior art does teach or suggest the limitation “generating a primary signature from the received signature, wherein the generating is implemented by hashing a concatenated value formed from the at least one private key and the signature received from the communications device”. Prior art does teach or suggest the limitation “conveying the primary signature to a communications system”.


Any claims not directly addressed are allowed on its virtue of dependency.

*Conclusion*

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy   
January 21, 2008

CHRISTOPHER REVAK  
PRIMARY EXAMINER

